MARKED UP COPY OF AMENDMENT PURSUANT TO 37 CFS § 1.121 (b)(1)(iii)

Page 1, line 3.

BACKGROUND [OF THE INVENTION]

Page 1, Line 4.

[Field of the Invention]

Page 1, line 5 to page 1, line 7.

This [invention] disclosure relates to cryptographic communications systems, and more particularly, to [an] a public key infrastructure that provides a master public key to enable authorized access to encrypted files.

Page 1, line 8.

[Description of the Related Art]

Page 3 line 1 to page 3, line 7.

The second class of cryptographic algorithms, i.e. asymmetric key algorithms, uses different cipher keys for encrypting and decrypting. The user makes the encryption key public and keeps the decryption key private, and it is not feasible to derive the private decryption key from the public encryption key. Thus, anyone who knows the public key of a particular user could encipher a message to that user, whereas only the user who is the owner of the private key corresponding to that public key could decipher the message.

Page 3, line 22 to page 4, line 10.

PKI allows users to append a digital signature to an unencrypted message. A digital signature encrypted with a private key uniquely identifies the sender and connects the sender to the exact message. When combined with a digital time stamp, the message can also be proved to have been sent at a certain time. To create a signature, the sender must put their message through a one-way "hash function" to create a fixed-length string of data that represents the content of the message. This hash value is encrypted using an encryption key, thereby creating the sender's digital signature. The signature is then attached to the message. When the recipient gets the message they use a key to decrypt the digital signature, producing a hash value. They then put the message through the same hash function the sender used to create a hash value and compare the hash value they have re-created with the hash value they decrypted from the digital signature. If the hash value the recipient re-creates matches the hash value sent with the message, they know that no-one has tampered with the message. If anyone has changed even one bit in the message, the hash value the recipient re-creates will be different. By using the key that belongs to the sender to decrypt the signature, the recipient knows that the message could only have been "signed" by the key holder. If it was signed by someone else the signature would not decrypt properly. This is how a digital signature [provide] provides integrity and authentication.

Page 4, line 24 to page 5, line 6.

With the aid of PKI it is thus possible to establish a secure line of communication with anyone who is using a compatible decryption system. Sender and receiver no longer need a secure way to agree on a shared key. If one user wishes to communicate with another, they exchange the plain text of their public keys using

compatible public-key cryptographic software. Each user then encrypts their outgoing messages with the other's public key and decrypts received messages with their own secret, private key. The security of PKI thus relies upon the security of the private key. [Since] Because a third party may send their own key claiming to be another sender, the usefulness of digital signature as an authenticating tool is limited by the ability of the recipient to ensure the authenticity of the key used to verify the signature. In order to rely on the authenticity of the public key, a user needs to get it from some source other than the user sending the message.

Page 6, line 25 to page 7, line 19.

SUMMARY [OF THE INVENTION]

In accordance with the present [invention] disclosure, there is provided [an] a data encryption and decryption system using public key infrastructure that allows an authorized third party to accept and decrypt the encrypted data as required without requiring a private key escrow. The [invention] disclosure utilizes a user private key, a user public key, a master private key, a master public key, and a session key generated by the system. The data is encrypted utilizing the session key. The session key is encrypted once utilizing the user public key and again utilizing the master public key. The encrypted data and the encrypted session keys are included in a data packet that is transmitted from one data processing system to another. The session key is decrypted utilizing the user private key. The data is decrypted utilizing the session key. When the authorized third party requires access to the data on the destination processing system, the session key is decrypted with the master private key and the data is decrypted with the session key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present [invention] disclosure may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

FIG. 1 is a block diagram of a typical data processing system with which the present [invention] disclosure may be utilized.

FIG. 2 is a block diagram of a typical encryption system according to the present [invention] disclosure.

FIG. 3 is a flowchart of the method for encrypting and decrypting data according to the present [invention] disclosure.

Page 7, line 23 to page 8, line 7.

Referring to Fig. 1, data processing system 114 includes a central processing unit (CPU) 120, main memory 122, mass storage interface 124, network interface 126, and input/output devices 128 all connected by system bus 130. Those skilled in the art will appreciate that this system encompasses all types of data processing systems: personal computers, midrange computers, mainframes, etc. Note that many additions, modifications, and deletions can be made to this data processing system 114 when used as a component of the present [invention] disclosure. Examples of I/O devices 128 that may be connected to system bus 130 for entering and receiving data include a computer display monitor, an input keyboard, a mouse, and a printer. Data processing system 114 may be one of many workstations connected to a local area network (LAN), a wide area network (WAN), or a global information network such as the Internet.

Page 9, line 25 to page 10, line 4.

System bus 128 allows data to be transferred among the various components of data processing system 114. Although data processing system 114 is shown to contain only a single main CPU 120 and a single system bus 128, those skilled in the art will appreciate that the present [invention] disclosure may be practiced using a data processing system that has multiple CPUs 120 and/or multiple busses 128. In addition, the interfaces that are used in the preferred embodiment may include separate, fully programmed microprocessors that are used to off-load computationally intensive processing from CPU 120, or may include input/output (I/O) adapters to perform similar functions.

Page 10, line 20 to page 12, line 6.

While the present [invention] disclosure is described in the context of a fully functional data processing system, those skilled in the art will appreciate that the present [invention] disclosure is capable of being distributed as an article of manufacture in a variety of forms, and that the present [invention] disclosure applies equally regardless of the particular type of signal bearing media used to actually carry out the distribution. Examples of signal bearing media include: recordable type media such as floppy disks and CD-ROM, transmission type media such as digital and analog communications links, as well as other known media storage and distribution systems.

Fig. 2 shows a diagram of one embodiment of the present [invention] disclosure for a computer-based public key data encryption system 200 for secure communication between first data processing system 202 and second data processing system 204 that allows an authorized third party to gain access to encrypted files without the overhead of placing additional information in escrow. As shown in Fig. 2, the first user's private key 206 [are] is stored in second data processing system 204 for encrypting information sent by the second user to the first user. Certificate 208 includes data pertaining to the first user including the first user's public key 210, master

public key 212, and other information about the first user's public key 214 and the certifying authority 216. While Fig. 2 shows data for only one user, second data processing system 204 may store or have access to certificate information for every user with which encrypted information is exchanged.

In order to transmit a message to the first user on first data processing system 202, second data processing system 204 includes program instructions to generate session key 218, to encrypt data 220 using session key 218, to encrypt session key 218 with first user's public key 210, to encrypt session key 218 with master public key 212, to generate data packet 222 including encrypted session keys 224, 226 and encrypted data 228, and to transmit data packet 222 to first data processing system 202. Note that data packets such as data packet 222 may be generated and transmitted to one or more different data processing systems instead of or in addition to first data processing system 202, using the appropriate user's public key, session key 218 or a new session key, and master public key 212. First data processing system 202 receives encrypted data [packet] 228, and includes program instructions to decrypt encrypted session key 224 with first user's private key 206, and to decrypt encrypted data 228 with session key 218 to re-create original data 220.

Note that the present [invention] disclosure also includes master public key 212 and master private key 230 to allow an authorized third party to gain access to encrypted data received by a user. The third party executes program instructions on first data processing system 202 to decrypt encrypted session key 224 using master private key 230, and to decrypt encrypted data 228 with session key 218 and to re-create original data 220. Thus, the present [invention] disclosure advantageously provides a system that allows non-repudiation to be established with only one key pair and simplifies key escrow procedures and the attendant database management overhead. Additionally, multiple master public keys can be created for designated multiple master key authorities. This would require all the designated authorities to

combine their master private keys to decrypt the session key, thereby further helping to ensure that the encrypted data is accessed only by authorized third parties.

Page 13, line 17 to page 14, line 5.

[Since] Because the asymmetric encryption algorithms can be relatively computationally intensive compared to symmetric encryption algorithms, it is much simpler and efficient to use an asymmetric algorithm to encrypt and decrypt a cipher key that may then be used to encrypt and decrypt data using a symmetric algorithm. Thus, the present [invention] disclosure may be implemented using an asymmetric encryption algorithm, a symmetric encryption algorithm, or a combination of an asymmetric and symmetric encryption algorithm. The embodiments of the present [invention] disclosure would then change accordingly, however, the important aspect is the inclusion of one or more master public keys and one or more master private keys to allow an authorized third party to access the encrypted data even when the user's private key is not accessible.

While the [invention has] embodiments have been described with respect to the embodiments and variations set forth above, these embodiments and variations are illustrative and the [invention] disclosure is not to be considered limited in scope to these embodiments and variations. For example, a user's private key or master key may be stored on a smart card, however, the private keys may also be stored on alternate computer readable mediums that are incorporated in data processing system 114. Accordingly, various other embodiments and modifications and improvements not described herein may be within the spirit and scope of the present [invention] disclosure, as defined by the following claims.

Page 20, line 5 to page 20, line 16.

The [invention] disclosure encrypts and decrypts data using public key infrastructure with and allows an authorized third party to access and decrypt the encrypted data as required without requiring private key escrow. The [invention] disclosure utilizes a user private key, a user public key, a master private key, a master public key, and a session key generated by the system. The data is encrypted utilizing the session key. The session key is encrypted once utilizing the user public key and again utilizing the master public key. The encrypted data and the encrypted session keys are included in a data packet that is transmitted from one data processing system to another. The session key is decrypted utilizing the user private key. The data is decrypted utilizing the session key. When the authorized third party requires access to the data on the destination processing system, the session key is decrypted with the master private key and the data is decrypted with the session key.